Jana Sotáková

Curriculum Vitæ Current as of September 21, 2023

L228, Science Park 123, 1098 XG Amsterdam j.s.sotakova@uva.nl , jana-sotakova.github.io

Academic Positions

2019–2023 QuSoft and ILLC, University of Amsterdam PhD student supervised by Christian Schaffner, Serge Fehr and Peter Bruin

Areas of Research

number theory and arithmetic geometry in cryptography (11T71, 14G50) isogeny-based cryptography, post-quantum cryptography quantum algorithms in cryptanalysis

Publications

Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic. Accepted at the LMFDB, Computation, and Number Theory conference (LuCaNT) 2023.

Cathy Li, Jana Sotáková, Emily Wenger, Mohamed Malhou, Evrard Garcelon, Francois Charton, and Kristin Lauter. SALSA PICANTE: a machine learning attack on LWE with binary secrets. *CCS* 2023.

Gustavo Banegas, Juliane Krämer, Tanja Lange, Michael Meyer, Lorenz Panny, Krijn Reijnders, Jana Sotáková, and Monika Trimoska. Disorientation faults in CSIDH. *EUROCRYPT* 2023.

Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the Decisional Diffie-Hellman Problem for Class Group Actions Using Genus Theory - Extended Version. In J. Cryptol. 35, 4 (Oct 2022).

Gustavo Banegas, Daniel J. Bernstein, Fabio Campos, Tung Chou, Tanja Lange, Michael Meyer, Benjamin Smith, Jana Sotáková. CTIDH: faster constant-time CSIDH. In *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2021, *Issue* 4, pages 351-387.

Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the Decisional Diffie-Hellman Problem for Class Group Actions Using Genus Theory. In *Advances in Cryptology – CRYPTO 2020*, LNCS vol. 12171, pp. 92–120.

Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. Explicit connections between supersingular isogeny graphs and Bruhat–Tits trees. In *Women in Numbers Europe III. Association for Women in Mathematics Series*, vol 24. Springer, 2021.

Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Jana Sotáková, and Travis Scholl. Adventures in Supersingularland. *Experimental Mathematics*, Taylor and Francis, 2021.

Education

2019–	QuSoft, ILLC at the University of Amsterdam PhD student, topic: quantum cryptanalysis of isogeny-based cryptography, advisors: Christian Schaffner, Serge Fehr, and Peter Bruin
2017-2019	University of California, Berkeley graduate student, supported in part by the Fulbright Student scholarship (2017/2018)
2015-2017	ALGANT Master Programme in Algebra, Geometry and Number theory Master of Science, joint degree at University of Regensburg and Leiden University graduated July 2017 (<i>cum laude, Sehr gut</i>) Thesis: Eta quotients and class invariants of imaginary quadratic fields (link)
2012-2015	Bachelor of Mathematics, Masaryk University The Department of Mathematics and Statistics, Faculty of Science graduated August 2015 with honours; bachelor thesis: The Number Field Sieve Method (link)
Spring 2015	Erasmus+ mobility The Mathematical Institute of Leiden University.

Awards

2020	Best Paper Award at Crypto 2020
2017/2018	Fulbright student scholarship
2015/2017	ALGANT master scholarship
2015	Prize of the Head of the Department of Mathematics and Statistics, Masaryk University
2010–2015	JCMM PPNS Scholarship for talented students

Talks (selected)

July 2023	Deuring for the People talk at the LuCaNT 2023, Providence, RI
April 2023	Salsa Picante AICrypt 2023
April 2022	CTIDH: constant time CSIDH ACCESS seminar talk
March 2022	Breaking DDH using genus theory Isogeny-based Cryptography, Birmingham
Sep 2021	CTIDH: constant time CSIDH recorded talk for CHES 2021
Mar 2021	Algebraic aspects of isogeny-based cryptography RTG seminar at the Clemson University
Oct 2020	Elliptic curves over finite fields and their endomorphism rings Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties
Jun 2020	Elliptic curves, isogenies, and endomorphism rings ANTS 2020 Summer School (video)

Conferences, summer schools, research visits (recent)

2023	Arithmetic, Geometry, Cryptography and Coding Theory Luminy, June 2023.
2023	Meta AI Seattle, Dec 2022-March 2023. Research intern with Kristin Lauter
2022	PCMI Graduate Summer School Pack City, July 2022. Teaching assisant for Kristin Lauter.
2021	Quantum Cryptanalysis Dagstuhl Seminar 21421, October 2021
2021	Supersingular Isogeny graphs in Cryptography BIRS workshop (online), August 23-27, 2021
2021	PCMI 2021 Graduate Summer School teaching assistant for Kristin Lauter, online school, July 2021
2021	Isogeny school online summer school, lecturer in Week 6, Summer 2021
2021	Supersingular Isogeny graphs in Cryptography BIRS workshop (online), August 23-27, 2021
2020	The Quantum Wave in computing (visitor) Simons Institute program on quantum computing, 3 week visit Jan-Feb 2020

Teaching

University of Amsterdam (as teaching assistant)

Spring 2023Computational complexity(teacher: Ronald de Haan)Spring 2022Information Theory(teacher: Leen Torenvliet)Fall 2021, 2020, 2019Modern Cryptography(teacher: Christian Schaffner)Fall 2020Mathematical Proof Methods for Logic(teacher: Julian Schlöder)

UC Berkeley (as graduate student instructor)

Spring 2019Math 16B Analytic Geometry and Calculus(teacher: Kelli Talaska)Fall 2018Math 16A Analytic Geometry and Calculus(teacher: Kelli Talaska)Spring 2018Math 1A Calculus(teacher: Richard Bamler)

Service

Spring 2021	I organized a reading group at QuSoft on quantum algorithms for isogeny problems
2020-2022	Women in Quantum Development, organizing committee member
2020-	Women in the Faculty mentoring program for students at UvA (mentor)
2019	The Noetherian Ring at UC Berkeley, organizer
2018–2019	Math Graduate Student Association officer at UC Berkeley

Skills

languages	English (C2), Dutch (C1), German (B1), Spanish (A2), Czech (native)
code	Python, C, Magma, Sage